Investigations dans/avec les noms de domaine/le DNS

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Investigations dans/avec les noms de domaine/le DNS

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

afnic

But de l'exposé

1. Expliquer comment trouver de l'information sur un nom de domaine

afnic

But de l'exposé

1. Expliquer comment trouver de l'information sur un nom de domaine
2. Expliquer comment utiliser le DNS pour récolter des informations

afnic

But de l'exposé

1. Expliquer comment trouver de l'information sur un nom de domaine
2. Expliquer comment utiliser le DNS pour récolter des informations
3. Public visé : toute personne qui, au cours d'une recherche, tombe sur un **nom de domaine** comme `www.example.com`

afnic

Quelques rappels

Quelques rappels

- Un nom de domaine est fait de **composants** séparés par des points. Le plus général est à droite.

Quelques rappels

- Un nom de domaine est fait de **composants** séparés par des points. Le plus général est à droite.
- `nca.x.gsi.gov.uk` a cinq composants. Le **TLD** (*Top-Level Domain*, `uk`) est à droite.

Quelques rappels

- Un nom de domaine est fait de **composants** séparés par des points. Le plus général est à droite.
- `nca.x.gsi.gov.uk` a cinq composants. Le **TLD** (*Top-Level Domain*, `uk`) est à droite.
- Des noms peuvent être **délégués** et on change alors d'organisme responsable. Par exemple `uk.com` est délégué depuis `com` et délègue à son tour. Rien dans le nom n'indique où est la frontière de délégation : il faut utiliser le DNS

afnic

L'industrie des noms de domaine

- Il y a au moins deux acteurs, le **titulaire** (*registrant*) du nom et le **registre** (*registry*).

L'industrie des noms de domaine

- Il y a au moins deux acteurs, le **titulaire** (*registrant*) du nom et le **registre** (*registry*).
- Dans certains cas, l'enregistrement ne se fait pas en direct mais via un troisième acteur, le **bureau d'enregistrement** (BE, *registrar*). C'est le système RRR (*registry-registrar-registrant*).

afnic

L'industrie des noms de domaine

- Il y a au moins deux acteurs, le **titulaire** (*registrant*) du nom et le **registre** (*registry*).
- Dans certains cas, l'enregistrement ne se fait pas en direct mais via un troisième acteur, le **bureau d'enregistrement** (BE, *registrar*). C'est le système RRR (*registry-registrar-registrant*).
- Les serveurs DNS du nom sont parfois gérés par le titulaire, parfois par le BE, parfois par un hébergeur DNS.

afnic

Mince ou épais

Mince ou épais

- `fr` est un registre épais : les informations sociales (nom des titulaires et contacts, adresses, téléphone. . .) sont stockées dans une base de données du **registre**.

Mince ou épais

- `fr` est un registre épais : les informations sociales (nom des titulaires et contacts, adresses, téléphone. . .) sont stockées dans une base de données du **registre**.
- `com` est un registre mince : les informations sociales sont dans une base du **BE**. Le registre a juste les informations techniques. Dans une investigation, il faut interroger **les deux**.

afnic

Outils à utiliser

On peut interroger les bases du réseau depuis :

Outils à utiliser

On peut interroger les bases du réseau depuis :

1. Un logiciel client local à sa machine,

Outils à utiliser

On peut interroger les bases du réseau depuis :

1. Un logiciel client local à sa machine,
2. Un logiciel situé chez un tiers (le fameux *cloud*).

afnic

Outils à utiliser

On peut interroger les bases du réseau depuis :

1. Un logiciel client local à sa machine,
2. Un logiciel situé chez un tiers (le fameux *cloud*).

Le problème n'est pas « logiciel graphique » vs. « ligne de commande »

Il est « logiciel sur **votre** machine » vs. « chez un tiers ». La difficulté de ces enquêtes vient de l'interprétation, pas du logiciel.

afnic

Problèmes avec un site tiers

Problèmes avec un site tiers

1. On ajoute un acteur, qui peut modifier/masquer des données

Problèmes avec un site tiers

1. On ajoute un acteur, qui peut modifier/masquer des données
2. Il peut aussi savoir ce qu'on fait. Dans une enquête sensible, ce manque de vie privée peut être grave.

afnic

Problèmes avec un site tiers

1. On ajoute un acteur, qui peut modifier/masquer des données
2. Il peut aussi savoir ce qu'on fait. Dans une enquête sensible, ce manque de vie privée peut être grave.
3. Les informations peuvent être du code JavaScript et un site Web peut donc être victime d'un XSS.

afnic

Interroger les bases sociales

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web

afnic

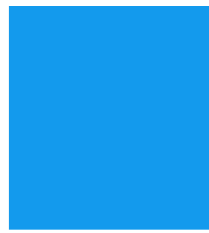
Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web
- Les bons clients whois trouvent automatiquement le serveur (pas trivial)

afnic

Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web
- Les bons clients whois trouvent automatiquement le serveur (pas trivial)
- Rappel : les bases sont purement déclaratives et leur valeur varie...



Interroger les bases sociales

- Protocole whois : interrogation des bases des registres et BE
- Registres et BE fournissent également souvent une interface Web
- Les bons clients whois trouvent automatiquement le serveur (pas trivial)
- Rappel : les bases sont purement déclaratives et leur valeur varie...
- whois remplacé dans le futur ? Par RDAP ?mo

afnic

Démo whois

```
% whois cecyf.fr
...
%% This is the AFNIC Whois server.
...
status:       ACTIVE
holder-c:     C30672-FRNIC
...
nic-hdl:      C30672-FRNIC
type:         ORGANIZATION
address:      C/ centre de recherches de l'Eogn
address:      49, rue de Babylone
```

Clients whois

Clients whois

- Ligne de commande : `whois` sur Linux et FreeBSD (pas le même logiciel).

afnic

Clients whois

- Ligne de commande : `whois` sur Linux et FreeBSD (pas le même logiciel).
- Graphiques : Greenwich (Unix). NetTool (Unix) est bien plus pauvre. WhoisThisDomain (Windows)

Bases sociales pour les adresses IP

Auprès d'un des cinq RIR (registres d'adresses IP)

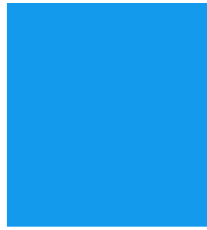
```
% whois 178.175.135.122
% This is the RIPE Database query service.
...
inetnum:        178.175.128.0 - 178.175.255.255
netname:        MD-TRABIA-20100504
descr:          I.C.S. Trabia-Network S.R.L.
country:        MD
org:            ORG-ITS10-RIPE
...
organisation:   ORG-ITS10-RIPE
org-name:       I.C.S. Trabia-Network S.R.L.
org-type:       LIR
address:        str. V. Pircalab 52
address:        2012
address:        Chisinau
address:        MOLDOVA, REPUBLIC OF
```

afnic

Interroger le DNS

Interroger le DNS

- Par défaut, on interroge son propre résolveur (géré par le FAI ou par le service informatique local)



Interroger le DNS

- Par défaut, on interroge son propre résolveur (géré par le FAI ou par le service informatique local)
- On peut aussi interroger directement les serveurs faisant autorité (utile s'il y a eu des changements récents)

afnic

Clients DNS

Clients DNS

- Ligne de commande : dig sur Unix (nslookup a trop de manques)

Clients DNS

- Ligne de commande : dig sur Unix (nslookup a trop de manques)
- Graphique : gresolver (Unix), NetTool (Unix, très pauvre), DNSdataView (Windows)

afnic

Démo DNS

```
% dig A www.cecyf.fr
...
;; ANSWER SECTION:
www.cecyf.fr. 10800 IN CNAME gpaas14.dc0.gandi.net.
gpaas14.dc0.gandi.net. 1800 IN A 217.70.180.154

%  dig A www.slate.fr
...
;; ANSWER SECTION:
www.slate.fr. 1344 IN A 190.93.243.33
www.slate.fr. 1344 IN A 141.101.123.33
www.slate.fr. 1344 IN A 190.93.240.33
www.slate.fr. 1344 IN A 190.93.241.33
www.slate.fr. 1344 IN A 190.93.242.33
```

(On note que tous les serveurs de Slate sont chez CloudFlare, qui « masque » le vrai hébergeur)

afnic

DNS historique

DNS historique

- Les commandes plus haut donnent l'état **actuel** du DNS

DNS historique

- Les commandes plus haut donnent l'état **actuel** du DNS
- Mais il existe des services qui enregistrent les réponses DNS et permettent ensuite de naviguer dans l'historique

afnic

DNS historique

- Les commandes plus haut donnent l'état **actuel** du DNS
- Mais il existe des services qui enregistrent les réponses DNS et permettent ensuite de naviguer dans l'historique
- DNSDB, CIRCL Passive DNS, passivedns.cn. . .

afnic

Exemple dans l'histoire

Le piratage du New York Times par la SEA (*Syrian Electronic Army*) se voit toujours sur DNSDB :

```
bailiwick nytimes.com.
count 122
first seen 2013-08-27 20:20:13 -0000
last seen 2013-08-28 03:18:15 -0000
nytimes.com. A 141.105.64.37
```

afnic

Pièges du DNS

Pièges du DNS

- Le DNS repose largement sur des **caches** (mémoire des informations déjà vues). L'information n'est pas toujours à jour.

Pièges du DNS

- Le DNS repose largement sur des **caches** (mémoire des informations déjà vues). L'information n'est pas toujours à jour.
- Les détournements de noms sont relativement fréquents (mot de passe au BE trop faible, par exemple). Un nom n'est pas toujours créé avec l'autorisation du titulaire.

afnic

Un exemple récent

Un exemple récent

- « Vous avez une démarche à accomplir cliquez sur le lien intitulé Pour régler votre impayé, `http://mobile.free.assistances.mobi/` »

afnic

Un exemple récent

- « Vous avez une démarche à accomplir cliquez sur le lien intitulé Pour régler votre impayé, `http://mobile.free.assistances.mobi/` »
- `whois assistances.mobi` $\longrightarrow$ adresse en France, sans doute fausse

afnic

Un exemple récent

- « Vous avez une démarche à accomplir cliquez sur le lien intitulé Pour régler votre impayé, `http://mobile.free.assistances.mobi/` »
- `whois assistances.mobi` $\longrightarrow$ adresse en France, sans doute fausse
- `dig A mobile.free.assistances.mobi` $\longrightarrow$ `94.23.151.40`

afnic

Un exemple récent

- « Vous avez une démarche à accomplir cliquez sur le lien intitulé Pour régler votre impayé, `http://mobile.free.assistances.mobi/` »
- `whois assistances.mobi` $\longrightarrow$ adresse en France, sans doute fausse
- `dig A mobile.free.assistances.mobi` $\longrightarrow$ `94.23.151.40`
- `whois 94.23.151.40` $\longrightarrow$ OVH

Un exemple récent

- « Vous avez une démarche à accomplir cliquez sur le lien intitulé Pour régler votre impayé, `http://mobile.free.assistances.mobi/` »
- `whois assistances.mobi` $\longrightarrow$ adresse en France, sans doute fausse
- `dig A mobile.free.assistances.mobi` $\longrightarrow$ `94.23.151.40`
- `whois 94.23.151.40` $\longrightarrow$ OVH
- Recherche DNSDB sur `94.23.151.40` $\longrightarrow$ Plein de domaines

afnic

Conclusion

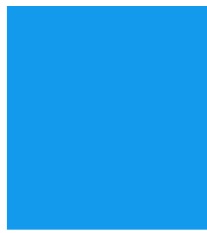
Conclusion

1. Méfiez-vous des sites Web tiers (confidentialité et intégrité),

afnic

Conclusion

1. Méfiez-vous des sites Web tiers (confidentialité et intégrité),
2. Soyez prudent dans l'interprétation, il y a des pièges,



Conclusion

1. Méfiez-vous des sites Web tiers (confidentialité et intégrité),
2. Soyez prudent dans l'interprétation, il y a des pièges,
3. Pratiquez régulièrement pour bien connaître vos outils et leurs limites.

afnic

Merci !

www.afnic.fr
contact@afnic.fr